(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年5 月10 日 (10.05.2002)

PCT

(10) 国際公開番号
WO 02/37285 A1

(51) 国際特許分類[7]: G06F 12/14, G09G 5/00, H04N 7/16, 1/00, 1/44

(21) 国際出願番号: PCT/JP01/09279

(22) 国際出願日: 2001 年10 月23 日 (23.10.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-331533
2000 年10 月30 日 (30.10.2000) JP
特願2001-112042 2001 年4 月10 日 (10.04.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ザインエレクトロニクス株式会社 (THINE ELECTRONICS, INC.) [JP/JP]; 〒104-0032 東京都中央区八丁堀1丁目10番7号 マツダ八重洲通ビル6階 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 挟間克樹 (HAZAMA, Katsuki) [JP/JP]. 桑山克己 (KUWAYAMA, Katsumi) [JP/JP]; 〒104-0032 東京都中央区八丁堀1丁目10番7号 マツダ八重洲通ビル6階 ザインエレクトロニクス株式会社内 Tokyo (JP).

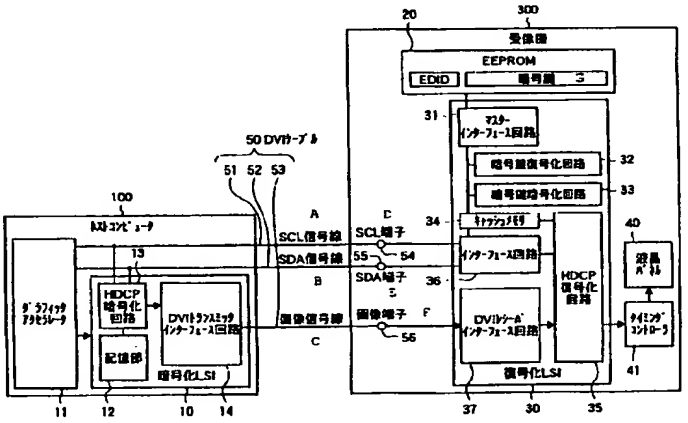
(81) 指定国 (国内): CA, CN, IL, IN, JP, KR, RU, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[続葉有]

(54) Title: SEMICONDUCTOR INTEGRATED CIRCUIT, RECEIVER APPARATUS USING THE SAME, RECEIVER APPARATUS MANUFACTURING METHOD AND REPAIRING METHOD, AND VIDEO PROVIDING METHOD

(54) 発明の名称: 半導体集積回路、それを用いた受信側装置、受信側装置の製造方法及び修理方法、並びに、画像提供方法



100...HOST COMPUTER
10...ENCRYPTING LSI
11...GRAPHIC ACCELERATOR
13...HDCP ENCRYPTING CIRCUIT
12...STORING UNIT
14...DVI TRANSMITTER INTERFACE CIRCUIT
50...DVI CABLES
A...SCL SIGNAL LINE
B...SDA SIGNAL LINE
C...VIDEO SIGNAL LINE
D...SCL TERMINAL
E...SDA TERMINAL
F...VIDEO TERMINAL
300...RECEIVER
G...ENCRYPTION KEY
30...DECRYPTING LSI
31...MASTER INTERFACE CIRCUIT
32...ENCRYPTION KEY DECRYPTING CIRCUIT
33...ENCRYPTION KEY ENCRYPTING CIRCUIT
34...CACHE MEMORY
36...INTERFACE CIRCUIT
37...DVI RECEIVER INTERFACE CIRCUIT
35...HDCP DECRYPTING CIRCUIT
40...LIQUID CRYSTAL PANEL
41...TIMING CONTROLLER

(57) Abstract: In a receiver or the like for reproducing encrypted video signals, a semiconductor integrated circuit wherein the number of the components used therein has been reduced and wherein, after completion of the receiver hardware, information can be written into a nonvolatile memory and the written information cen be rewritten. This semiconductor integrated circuit is one for use in an apparatus for receiving encrypted video signals and has an interface circuit for effecting a serial communication with the exterior and also has a memory control circuit for controlling the nonvolatile memory to write and/or read a first information

WO 02/37285 A1

[続葉有]

添付公開書類:
— 国際調査報告書

to be transmitted to the exterior by the interface circuit and a second information to be used to decrypt the encrypted video signals.

(57) 要約:

暗号化された画像信号を再生する受像機等において、使用する部品点数を減らすことができ、且つ、受像機のハードウエア完成後に、不揮発性メモリに情報を書き込んだり、書き込まれた情報を書き換えることができる半導体集積回路。この半導体集積回路は、暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、外部とシリアル通信を行うインターフェース回路と、インターフェース回路によって外部に送信される第１の情報、及び、暗号化された画像信号を復号化するために用いられる第２の情報を書き込み、及び／又は、読み出すように不揮発性メモリを制御するメモリ制御回路とを具備する。

明　細　書

半導体集積回路、それを用いた受信側装置、受信側装置の製造方法及び修理方法、並びに、画像提供方法

技術分野

本発明は、一般的に半導体集積回路に関し、特に、暗号化された画像信号を受信又は送信するために用いる半導体集積回路に関する。また、本発明は、受信用の半導体集積回路を用いた受像機等の受信側の装置、受信側の装置の製造方法及び修理方法に関する。さらに、本発明は、そのような受像機を用いた画像提供方法に関する。

背景技術

パーソナルコンピュータ等の送信側の装置とモニタやプロジェクタ等の受信側の装置との接続に関するＤＤＣ（display data channel）と呼ばれる規格は、受信側の装置が、送信側の装置から、その受信側の装置にとって最適の信号を得られるように定められている。

ＤＤＣ規格に従う受像機は、ＥＤＩＤ（extended display identification data）と呼ばれる情報が記憶されたＥＥＰＲＯＭ（electrically erasable programmable read-only memory）を有している。ＥＤＩＤには、受像機の種類、表示できる解像度、クロック周波数、メーカー名、シリアル番号等の情報が含まれている。また、ＥＤＩＤを記憶するＥＥＰＲＯＭとしては、２線式シリアルＥＥＰＲＯＭが一般的に用いられ、Ｉ²Ｃバス方式に準ずるシリアル通信によってデータが送受信される（Ｉ²Ｃバスは、フィリップス社の登録商標）。

このシリアル通信においては、ＳＤＡ（シリアルデータ）端子及びＳ

ＣＬ（シリアルクロック）端子と呼ばれる２つの端子を用いて、受像機に内蔵されているＥＥＰＲＯＭの制御と情報の送受信が行われる。受像機のＳＤＡ端子及びＳＣＬ端子がケーブルを介してパーソナルコンピュータに接続されると、パーソナルコンピュータは、ＥＥＰＲＯＭに記憶されているＥＤＩＤを読み取ることができる。これにより、受像機にとって最適な信号に関する情報が、パーソナルコンピュータに提供される。

一方、パーソナルコンピュータ等から受像機に送信される画像信号は、アナログ信号からデジタル信号に移行しつつあり、画像信号の劣化がほとんど起こらないようになってきた。このため、画像信号の不法なコピー等から著作物を保護する必要が生じている。そのための手段の１つとして、パーソナルコンピュータ等から受像機に送信される画像信号を暗号化することが行われている。その中でも、現在、ＨＤＣＰ（high-bandwidth digital content protection）と呼ばれる方式が標準になりつつある。

図１は、ＨＤＣＰ方式による従来の受像機を用いた画像伝送システムを示すブロック図である。図１に示すように、この画像伝送システムは、ホストコンピュータ１００と受像機２００とによって構成される。受像機２００は、ＨＤＣＰ方式による暗号鍵情報（以下、「暗号鍵」ともいう）を保有する。暗号鍵は、受像機２００からＤＤＣによってホストコンピュータ１００に通知される「公開鍵」と、不特定多数に知られてはならない「秘密鍵」とを含んでいる。

ホストコンピュータ１００は、高速で描画するための画像信号を生成するグラフィックアクセラレータ１１と、ＨＤＣＰ方式による暗号化ＬＳＩ１０とを含んでいる。暗号化ＬＳＩ１０は、暗号鍵を記憶する記憶部１２と、記憶部１２に記憶されている暗号鍵を用いて画像信号を暗号

化するＨＤＣＰ暗号化回路１３と、画像信号の送信を行うＤＶＩトランスミッタインターフェース回路１４とを有している。ＨＤＣＰ方式においては、一般的に、画像信号の送受信にＤＶＩ（digital visual interface）規格が用いられているので、画像信号を送信する回路及び受信する回路は、ＤＶＩ規格に準拠している。

一方、受像機２００は、ＥＤＩＤを記憶するシリアルＥＥＰＲＯＭ２２１と、暗号鍵を記憶するＥＥＰＲＯＭ２２２と、ＨＤＣＰ方式によって暗号化された画像信号を暗号鍵を用いて復号化する半導体集積回路（復号化ＬＳＩ）２３０と、液晶パネル２４０と、タイミングコントローラ２４１とを含んでいる。

復号化ＬＳＩ２３０は、ＥＥＰＲＯＭ２２２を制御するマスターインターフェース回路２３１と、ＨＤＣＰ復号化回路２３５と、暗号鍵等の送受信を行うインターフェース回路２３６と、画像信号の受信を行うＤＶＩレシーバインターフェース回路２３７とを有している。

液晶パネル２４０は、復号化された画像信号に基づいて画像を表示する。また、タイミングコントローラ２４１は、液晶パネルの信号線に画像信号を入力するタイミングをコントロールする。

さらに、受像機２００は、ＥＥＰＲＯＭ２２１及びインターフェース回路２３６に接続されたＳＣＬ端子５４及びＳＤＡ端子５５と、ＤＶＩレシーバインターフェース回路２３７に接続された画像端子５６とを有しており、これらの端子に接続されたＤＶＩケーブル５０を通じて外部の機器と信号の送受信を行う。ＤＶＩケーブル５０は、ＤＤＣ規格によるデータの送受信に用いられるＳＣＬ信号線５１、ＳＤＡ信号線５２及び画像信号線５３を含んでいる。

システムが起動されると、ホストコンピュータ１００は、受像機２００のＥＥＰＲＯＭ２２１に記憶されているＥＤＩＤと、ＥＥＰＲＯＭ２

２２に記憶されている公開鍵とを読み出すことができる。ホストコンピュータ１００において、グラフィックアクセラレータ１１は、受信されたＥＤＩＤに基づいて、受像機２００に適した画像信号を生成する。また、受信された公開鍵に基づいて受像機２００が認証された場合に、ＨＤＣＰ暗号化回路１３は、暗号鍵を用いて画像信号を暗号化し、ＤＶＩトランスミッタインターフェース回路１４は、これを受像機２００に送信する。

受像機２００において、マスターインターフェース回路２３１は、ＥＥＰＲＯＭ２２２から暗号鍵を読み出して、ＨＤＣＰ復号化回路２３５に供給する。ＨＤＣＰ復号化回路２３５は、この暗号鍵を用いて、ＤＶＩレシーバインターフェース回路２３７によって受信された画像信号を復号化する。復号化された画像信号は、タイミングコントローラ２４１の制御の下で、液晶パネル２４０に表示される。

このような画像伝送システムにおいて、受像機２００のＥＥＰＲＯＭ２２２に記憶されている公開鍵と秘密鍵とを含む暗号鍵の内、秘密鍵は不特定多数に知られてはならない。従って、パーソナルコンピュータ等によって自由に読み出すことができるＥＤＩＤと、読み出しに制限を加えなくてはならない暗号鍵とを、同じＥＥＰＲＯＭに保存することはできなかった。そのため、従来は、ＤＤＣ用の信号線に接続されたシリアルＥＥＰＲＯＭ２２１にＥＤＩＤのみを記憶させて、暗号鍵を記憶するためのＥＥＰＲＯＭ２２２を別に用意していた。画像信号を復号化する復号化ＬＳＩ２３０は、ＥＥＰＲＯＭ２２２を制御して暗号鍵を読み出し、パーソナルコンピュータ等からの要求に応じて公開鍵のみをＤＤＣ用の信号線に提供していた。

ところで、暗号鍵を保存するＥＥＰＲＯＭ２２２は、ＤＤＣ用の端子であるＳＣＬ端子５４及びＳＤＡ端子５５には接続されていないものの

、汎用のＥＥＰＲＯＭであるため、ＲＯＭリーダー／ライター等を用いることにより簡単にその内容を読み出すことができる。従って、暗号鍵が平文のままＥＥＰＲＯＭ２２２に記憶されると、一般にその内容を明らかにされる恐れがあった。そこで、暗号鍵が読み出されることを防ぐため、ＥＥＰＲＯＭ２２２と復号化ＬＳＩ２３０との間をモールド樹脂等で封印する方法が提案されている。

しかしながら、このような方法を採ったとしても、依然としてＥＤＩＤを記憶するＥＥＰＲＯＭと暗号鍵を記憶するＥＥＰＲＯＭとの２個のＥＥＰＲＯＭが必要であり、部品点数の増加に伴うコストの上昇は避けられない。また、ＥＤＩＤと暗号鍵という２種類の情報を別個にそれぞれのＥＥＰＲＯＭに記憶させなくてはならないため、受像機の製造過程において、情報を記憶させる工程及びテスト工程が複雑となり、コストがかかっていた。さらに、ＥＥＰＲＯＭに暗号鍵を平文のまま書き込み、それを読み出すことができないように樹脂等で封印すると、故障等によりＥＥＰＲＯＭを再度書き換える必要が生じても、ＥＥＰＲＯＭを書き換えることが不可能になってしまうという欠点があった。

発明の開示

そこで、上記の点に鑑み、本発明の第１の目的は、暗号化された画像信号を受信する受像機等の受信側の装置において使用する部品点数を減らすことができ、且つ、ハードウエアの完成後に不揮発性メモリに情報を再度書き込むことを可能とする半導体集積回路を提供することである。また、本発明の第２の目的は、受信側の装置に画像信号を送信する送信側の装置においてセキュリティを向上させることができる半導体集積回路を提供することである。さらに、本発明の第３の目的は、上記のような受信用の半導体集積回路を用いた受信側の装置を提供することであ

る。加えて、本発明の第４の目的は、受像機を用いた画像提供方法を実現することである。

以上の課題を解決するため、本発明の第１の観点に係る半導体集積回路は、暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、外部とシリアル通信を行うインターフェース回路と、インターフェース回路によって外部に送信される第１の情報、及び、暗号化された画像信号を復号化するために用いられる第２の情報を書き込み、及び／又は、読み出すように不揮発性メモリを制御するメモリ制御回路とを具備する。

また、本発明の第２の観点に係る半導体集積回路は、暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化回路と、暗号鍵復号化回路によって復号化された暗号鍵を用いて画像信号を復号化する画像信号復号化回路とを具備する。

さらに、本発明の第３の観点に係る半導体集積回路は、画像信号を暗号化して受信側の装置に送信する装置において用いるための半導体集積回路であって、画像信号に所定の信号処理を施す画像処理回路と、所定の信号処理が施されていない画像信号と所定の信号処理が施された画像信号との内の一方を選択する選択回路と、選択回路によって選択された画像信号を暗号化する暗号化回路と、受信側の装置から受信した暗号鍵に基づいて受信側の装置を認証するか否かについて判断し、受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように選択回路及び暗号化回路を制御し、受信側の装置が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように選択回路及び暗号化回路を制御する制御回路とを具備する。

本発明の１つの観点に係る受信側の装置は、暗号化された画像信号を受信する装置であって、外部とシリアル通信を行う第１の手段と、暗号化された画像信号を受信する第２の手段と、第１の手段によって外部に送信される第１の情報、及び、第２の手段によって受信された画像信号を復号化するために用いられる第２の情報を記憶するための不揮発性メモリと、不揮発性メモリに記憶されている第２の情報を用いて、第２の手段によって受信された画像信号を復号化する第３の手段とを具備する。

本発明の１つの観点に係る製造方法は、外部とシリアル通信を行う第１の手段と、暗号化された画像信号を受信する第２の手段と、不揮発性メモリとを有し、暗号化された画像信号を受信する装置を製造する方法であって、第１の手段を用いてシリアル通信を行うことにより、装置に関する第１の情報、及び、第２の手段によって受信された画像信号を復号化するために用いられる第２の情報を装置に入力するステップ（ａ）と、ステップ（ａ）において入力された第１及び第２の情報を不揮発性メモリに書き込むステップ（ｂ）とを具備する。

本発明の１つの観点に係る画像提供方法は、暗号鍵を入力する第１の手段と、暗号化された画像信号を受信する第２の手段とを有し、暗号化された画像信号を受信して画像を表示する受像機を用いて画像を提供する方法であって、第１の手段によって受像機に入力された暗号鍵に基づいて、第１の手段によって受像機に入力された暗号鍵に基づいて、受像機を認証するか否かについて判断するステップ（ａ）と、ステップ（ａ）において受像機が認証された場合に、第２の手段によって受信された画像信号を第１の手段によって受像機に入力された暗号鍵を用いて復号化し、復号化された画像信号に基づいて画像を表示するステップ（ｂ）とを具備する。

本発明によれば、受信用の半導体集積回路において、ＥＤＩＤと暗号鍵とを１つの不揮発性メモリに記憶させるので、受像機等の受信側の装置に用いられる部品点数を削減することができると共に、受信側の装置の製造過程における情報の書き込み工程及びテスト工程を簡略化することができる。また、ハードウエアの完成後に不揮発性メモリに情報を書き込んだり、書き換えることができるので、受信側の装置の製造が容易であり、出荷後に故障が起きても受信側の装置を修理することができる。さらに、暗号鍵を入力する第１の手段を有する受像機を用いることにより、暗号鍵を有する特定のユーザのみに画像を提供する画像提供方法を実現することができる。

また、本発明によれば、送信用の半導体集積回路において、受信側の装置を認証するか否かを判断し、認証しない場合には画質を劣化させる等の処理を行うので、外部のソフトウエアの助けを必要とせず、セキュリティを向上させることができる。

図面の簡単な説明

本発明の利点及び特徴は、以下の詳細な説明と図面とを関連させて考察すれば明らかになる。これらの図面において、同じ参照番号は同じ構成要素を指している。

図１は、従来の受像機を用いた画像伝送システムを示すブロック図である。

図２は、本発明の第１の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。

図３は、本発明の第１の実施形態に係る受信側の装置の変形例を用いた画像伝送システムを示すブロック図である。

図４は、本発明の第１の実施形態に係る受信側の装置において不揮発

性メモリにＥＤＩＤを書き込む動作を示すフローチャートである。

図５は、本発明の第１の実施形態に係る受信側の装置において不揮発性メモリに暗号鍵を書き込む動作を示すフローチャートである。

図６は、本発明の第１の実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

図７は、本発明の第２の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。

図８は、本発明の第２の実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

図９は、本発明の第１の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。

図１０は、本発明の第２の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。

発明を実施するための最良の形態

図２は、本発明の第１の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。以下の実施形態においては、受信側の装置として、液晶パネル等の表示装置を有する受像機を用いる場合について説明するが、表示装置を受信側の装置に含めない構成として、受信側の装置に外部の表示装置を接続するようにしても良い。

図２に示すように、この画像伝送システムは、ホストコンピュータ１００と受像機３００とによって構成される。受像機３００は、ＨＤＣＰ方式による暗号鍵を保有する。暗号鍵は、受像機３００からＤＤＣによってパーソナルコンピュータ１００に通知される公開鍵と、不特定多数に知られてはならない秘密鍵とを含んでいる。

ホストコンピュータ１００は、高速で描画するための画像信号を生成

するグラフィックアクセラレータ１１と、暗号化ＬＳＩ１０とを含んでいる。暗号化ＬＳＩ１０は、暗号鍵を記憶する記憶部１２と、記憶部１２に記憶されている暗号鍵を用いて画像信号を暗号化するＨＤＣＰ暗号化回路１３と、ＤＶＩ規格に従って画像信号の送信を行うＤＶＩトランスミッタインターフェース回路１４とを有している。。

ホストコンピュータ１００には、ＳＣＬ信号線５１と、ＳＤＡ信号線５２と、画像信号線５３とを含むＤＶＩケーブル５０を介して、受像機３００が接続されている。

受像機３００は、ＥＤＩＤ及び暗号鍵を記憶する不揮発性メモリとしてＥＥＰＲＯＭ２０と、ＨＤＣＰ方式によって暗号化された画像信号を暗号鍵を用いて復号化する半導体集積回路（復号化ＬＳＩ）３０と、復号化された画像信号に基づいて画像を表示するデバイスとして液晶パネル４０と、液晶パネルの信号線に画像信号を入力するタイミングをコントロールするタイミングコントローラ４１とを含んでいる。なお、不揮発性メモリとしては、シリアルＥＥＰＲＯＭ、パラレルＥＥＰＲＯＭ、フラッシュＥＥＰＲＯＭの他に、一般的なＰＲＯＭや電池内蔵のＳＲＡＭ等を用いることができる。また、画像を表示するデバイスとしては、液晶パネル４０の他に、ＰＤＰ（plasma display panel）やＣＲＴ（cathode ray tube）を用いても良い。

復号化ＬＳＩ３０は、ＥＥＰＲＯＭ２０を制御するマスターインターフェース回路３１と、暗号鍵復号化回路３２と、暗号鍵暗号化回路３３と、キャッシュメモリ３４と、暗号鍵等の送受信を行うインターフェース回路３６と、画像信号の復号化を行うＨＤＣＰ復号化回路３５と、画像信号の受信を行うＤＶＩレシーバインターフェース回路３７とを内蔵している。なお、復号化ＬＳＩ３０がＥＥＰＲＯＭ２０等の不揮発性メモリを内蔵するようにしても良い。あるいは、ＨＤＣＰ復号化回路３５

及びＤＶＩレシーバインターフェース回路３７と、それ以外の回路とを、別個の半導体集積回路に形成しても良い。

インターフェース回路３６は、ＥＤＩＤや暗号鍵等の情報の送受信を制御する。また、インターフェース回路３６は、I^2Cバス方式による通信において、スレーブデバイスとして動作する。インターフェース回路３６は、ＳＣＬ端子５４及びＳＤＡ端子５５に接続されており、ＳＣＬ信号線５１及びＳＤＡ信号線５２を介して外部との信号の送受信を行う。

キャッシュメモリ３４は、ＥＥＰＲＯＭ２０に書き込まれる情報を一時的に保存したり、ＥＥＰＲＯＭ２０から読み出された情報を一時的に保存する。キャッシュメモリ３４としては、ＳＲＡＭ（static random access memory）を用いることができる。

暗号鍵暗号化回路３３は、平文で入力された暗号鍵を暗号化する。暗号化された暗号鍵は、マスターインターフェース回路３１によってＥＥＰＲＯＭ２０に保存される。なお、暗号化された暗号鍵が復号化ＬＳＩ３０に入力される場合には、暗号鍵暗号化回路３３は不要である。

暗号鍵復号化回路３２は、暗号化された暗号鍵を平文に復号化する。復号化された暗号鍵は、暗号化された画像信号を復号化する際に用いられる。

マスターインターフェース回路３１は、ＥＥＰＲＯＭ２０との間における信号の送受信を制御し、ＥＥＰＲＯＭ２０に対して情報の書き込みや読み出しを行う。また、マスターインターフェース回路３１は、ＥＥＰＲＯＭ２０に書き込むべき情報と、ＥＥＰＲＯＭ２０に書き込まれた情報とを比較（ベリファイ）し、ＥＥＰＲＯＭ２０に書き込まれた内容の信頼性を高める動作モードを有している。この動作モードは、復号化ＬＳＩ３０のテストモードにおいて設定することができる。

ＥＥＰＲＯＭ２０に暗号化された暗号鍵が記憶されている場合には、暗号鍵復号化回路３２が、暗号化された暗号鍵を平文に復号化し、マスターインターフェース回路３１が、復号化された暗号鍵を入力された鍵と比較する。マスターインターフェース回路３１は、ＥＥＰＲＯＭ２０に情報が正しく書き込まれたか否かをチェックするために、エラー検出コード又はエラー訂正コードを計算してＥＥＰＲＯＭ２０に書き込まれた情報を検証するようにしても良い。

あるいは、図３に示すように、受像機４００において、フラッシュＥＥＰＲＯＭ６２を内蔵したマイクロコンピュータ６１を用いるようにしても良い。マイクロコンピュータ６１は、インターフェース回路３６又はキャッシュメモリ３４との間で信号の送受信を行い、内蔵するＥＥＰＲＯＭ６２に対して情報の書き込みや読み出しを行う。その場合には、復号化ＬＳＩ６０がマスターインターフェース回路を内蔵する必要はない。

再び図１を参照すると、ＨＤＣＰ復号化回路３５は、ＨＤＣＰ方式による暗号鍵を用いて、ＤＶＩレシーバインターフェース回路３７によって受信された画像信号を復号化する。

ＤＶＩレシーバインターフェース回路３７は、画像端子５６に接続されており、画像信号線５３を介してディジタル画像信号を受信する。ＤＶＩレシーバインターフェース回路３７は、ＤＶＩ規格に準拠しており、ＲＧＢ（赤、緑、青）の３つの画像信号チャンネルについて、エンコードされて送信されるシリアルデータをパラレルデータに変換する。

I^2Cバス方式による通信においては、それぞれのスレーブデバイスにスレーブアドレスが割り振られている。例えば、一般的に、ＥＤＩＤの送受信には、読み出し用としてアドレス「Ａ０ｈ」、書き込み用としてアドレス「Ａ１ｈ」が割り振られている。また、ＨＤＣＰ方式による

レシーバには、読み出し用としてアドレス「７６ｈ」、書き込み用としてアドレス「７７ｈ」が割り振られている。本実施形態におけるインターフェース回路３６は、ＨＤＣＰ方式によるレシーバに割り当てられているスレーブアドレス「７Ａｈ」及び「７Ｂｈ」と同様に、ＥＤＩＤの応答に割り当てられているスレーブアドレス「Ａ０ｈ」及び「Ａ１ｈ」を指定されたときにも応答するように設計されている。

一方、受像機のホスト側に用いられるＨＤＣＰ方式によるトランスミッタには、ＨＤＣＰ方式による暗号鍵等の送受信用としてアドレス「７８ｈ」及び「７９ｈ」、トランスミッタの物理層の設定用にアドレス「７０ｈ」及び「７１ｈ」が割り振られている。

次に、本実施形態に係る受信側の装置においてＤＤＣ規格によるＥＤＩＤを書き込む動作について、図２及び図４を参照しながら説明する。ＥＤＩＤを記憶するＥＥＰＲＯＭ２０においては、その誤動作を防ぐために、画像制御信号の１つであるＶＳＹＮＣ信号（vertical synchronizing signal：垂直同期信号）を用いることが一般的である。本実施形態においても、ＥＤＩＤの書込み及び読出しの制御においては、ＶＳＹＮＣ信号を併せて用いている。

図４は、本実施形態に係る受信側の装置において、不揮発性メモリにＥＤＩＤを書き込む動作を示すフローチャートである。この書き込み動作は、受信側の装置のハードウエアの完成後に行われる。

ステップＳ１０１において、ホストコンピュータ１００等の外部機器がスレーブアドレスＡ１ｈを指定してＥＤＩＤを送信すると、受像機３００の復号化ＬＳＩ３０は、ＳＣＬ端子５４及びＳＤＡ端子５５を用いてＥＤＩＤを受信する。

ステップＳ１０２において、インターフェース回路３６は、受信したＥＤＩＤをキャッシュメモリ３４に一旦保存する。

ステップＳ１０３において、マスターインターフェース回路３１は、キャッシュメモリ３４に保存された内容をＥＥＰＲＯＭ２０に書き込む。或いは、マスターインターフェース回路３１は、ＥＤＩＤをキャッシュメモリ３４から読み出しながら、並行してＥＥＰＲＯＭ２０にこれを書き込んでも良い。

次に、本実施形態に係る受信側の装置においてＨＤＣＰ方式による暗号鍵を書き込む動作について、図２及び図５を参照しながら説明する。

図５は、本実施形態に係る受信側の装置において、不揮発性メモリにＨＤＣＰ方式による暗号鍵を書き込む動作を示すフローチャートである。この書き込み動作も、受信側の装置のハードウエアの完成後に行われる。

ステップＳ２０１において、ホストコンピュータ１００等の外部機器がスレーブアドレス７７ｈを指定して暗号鍵を送信すると、受像機３００の復号化ＬＳＩ３０は、ＳＣＬ端子５４及びＳＤＡ端子５５を用いて暗号鍵を受信する。

ステップＳ２０２において、インターフェース回路３６は、受信した暗号鍵をキャッシュメモリ３４に一旦保存する。

ステップＳ２０３において、復号化ＬＳＩ３０は、キャッシュメモリ３４に保存されている暗号鍵について、暗号化が必要であるか否かを判断する。即ち、暗号鍵をＥＥＰＲＯＭ２０に平文のままで保存すると、暗号鍵が一般に漏れてしまう恐れがある。そこで、受像機の製造者は、暗号鍵を信頼性高く保存したい場合には、暗号鍵を暗号化してＥＥＰＲＯＭ２０に保存することができるようになっている。この暗号化のためには、復号化ＬＳＩ３０に内蔵されている暗号鍵暗号化回路３３を用いても良いし、予め暗号化されている暗号鍵を復号化ＬＳＩ３０に送信しても良い。

復号化ＬＳＩ３０内で暗号鍵を暗号化する場合には、ステップＳ２０４において、暗号鍵暗号化回路３３が暗号鍵を暗号化してからステップＳ２０５に移行する。このようにして、暗号鍵を暗号化するモードを設けることにより、受像機において暗号鍵を信頼性高く保存することができる。

ここで、暗号鍵の暗号化においては、画像信号の暗号化における暗号化強度と同等以上の暗号化強度が必要である。また、暗号鍵を暗号化するモードに移行する方法については、一般ユーザに理解されにくい方法が用いられ、これを公開しないことにより、暗号化のアルゴリズムを秘匿することができる。例えば、特殊なコマンドを復号化ＬＳＩ３０に入力したときに、暗号鍵暗号化回路３３が活性化されて、暗号鍵を暗号化するモードに移行するようにしても良い。そのような特殊なコマンドにおいても、画像信号を暗号化する際の暗号化強度と同等以上のセキュリティ性が必要である。

一方、あらかじめ暗号化された暗号鍵を受信した場合や、セキュリティ性があまり高くないため平文のまま保存しても構わない暗号鍵を受信した場合には、ステップＳ２０５に直接移行する。ステップＳ２０５において、マスターインターフェース回路３１が、暗号鍵をＥＥＰＲＯＭ２０に書き込む。

なお、ＥＤＩＤや暗号鍵をＥＥＰＲＯＭ２０に書き込む際に用いるデータフォーマットは、復号化ＬＳＩ３０で読み出すことが可能なデータフォーマットであれば良く、ＤＤＣ規格で定められたものと異なっていても構わない。例えば、エラー検出コード又はエラー訂正コードを含むデータフォーマットを用いても良い。

本実施形態によれば、以上述べたＥＤＩＤや暗号鍵を保存するためのＥＥＰＲＯＭを１つに集約することができる。また、ＨＤＣＰ方式によ

る暗号鍵を暗号化することにより、暗号鍵が保存されているＥＥＰＲＯＭ２０と復号化ＬＳＩ３０との間をモールドで固める必要がなくなる。受像機の製造工程において、ＥＤＩＤ及び暗号鍵の書き込みは、ハードウエアの完成後に、ＳＣＬ端子５４及びＳＤＡ端子５５を用いて行うことができる。また、受像機の出荷後にＥＥＰＲＯＭ２０の内容に不良が発見された場合に、修理作業としてＥＤＩＤ及び暗号鍵の書き込みを行うこともできる。

次に、本実施形態に係る受信側の装置を用いて画像を提供する方法について、図２及び図６を参照しながら説明する。図６は、本実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

まず、ステップＳ３０１において、受像機３００の電源を投入し、ステップＳ４０１において、ホストコンピュータ１００の電源を投入する。

受像機３００の電源が投入されると、受像機３００は、ステップＳ３０２において、ＥＥＰＲＯＭ２０に書き込まれたＥＤＩＤ及び暗号鍵を読み出してキャッシュメモリ３４に保存し、ホストコンピュータ１００からの要求に対応する準備を整える。この準備動作は、電源投入時に限らず、マイクロコンピュータ等の制御により行っても良い。

ホストコンピュータ１００は、ステップＳ４０２において、ＳＣＬ端子５４及びＳＤＡ端子５５を通じてＥＤＩＤのアドレスＡ０ｈ及びＡ１ｈを指定して、ＥＤＩＤの送信を要求する。これに応答して、受像機３００は、ステップＳ３０３において、キャッシュメモリ３４に保存されている情報を利用し、インターフェース回路３６を介して、あたかも復号化ＬＳＩ３０がＥＤＩＤ専用のＥＥＰＲＯＭであるかのような振る舞いをして、ＥＤＩＤをホストコンピュータ１００に送信する。ホストコ

ンピュータ１００は、ステップＳ４０３において、ＥＤＩＤを受信して受像機３００に関する情報を解読する。

なお、受像機３００の復号化ＬＳＩ３０は、電源が投入されていなくても、ホストコンピュータ１００からＥＤＩＤの送信を要求されたら、ＤＶＩケーブルを介してホストコンピュータ１００から供給される電源によって動作して、ＥＤＩＤを送信しなければならない。一般的に、ホストコンピュータは５Ｖの電源電圧を供給するが、復号化ＬＳＩの動作電圧は３．３Ｖであり、受像機において降圧回路が必要になる。また、利用できる電流は５０ｍＡが目安であり、復号化ＬＳＩをフルに動作させるとこの電流値をオーバーしてしまう。従って、受像機に電源が投入されていないときにＥＤＩＤを送信するためには、消費電流についての配慮も必要である。

受像機３００は、ステップＳ３０４において、暗号鍵が暗号化されているか否かを判断する。即ち、受像機３００の復号化ＬＳＩ３０は、ＥＰＲＯＭ２０から暗号鍵が読み出されると、暗号鍵が暗号化されているか否かを自動認識する。暗号鍵が暗号化されていると判断された場合には、ステップＳ３０５において、暗号鍵復号化回路３２が暗号鍵を復号化し、ステップＳ３０６において、復号化された暗号鍵をキャッシュメモリ３４に保存する。一方、暗号鍵が暗号化されていないと判断された場合には、ステップＳ３０６において、暗号鍵をそのままキャッシュメモリ３４に保存する。

ホストコンピュータ１００が、ステップＳ４０４において、ＳＣＬ端子５４及びＳＤＡ端子５５を用いてＨＤＣＰ方式による公開鍵等の情報を要求すると、受像機３００は、ステップＳ３０７において、キャッシュメモリ３４に保存されている情報を利用し、インターフェース回路３６を介してホストコンピュータ１００に公開鍵等の情報を送信する。こ

こで、インターフェース回路３６は、ＨＤＣＰ方式による秘密鍵を平文のままホストコンピュータ１００に送信することはなく、ＨＤＣＰ方式による秘密鍵が一般に公開されるリスクを低減している。

ホストコンピュータ１００は、ステップＳ４０５において、受像機３００から公開鍵を受信すると、ステップＳ４０６において、公開鍵に基づいて受像機３００を認証するか否かについて判断する。具体的には、ホストコンピュータ１００が、受信した公開鍵とホスト側の公開鍵とに基づいて、乱数と秘密鍵とを用いた演算を行い、演算結果が一致した場合に、受像機３００を認証する。

ホストコンピュータ１００は、受像機３００が認証された場合に、ステップＳ４０７において、画像信号の暗号化を行い、ステップＳ４０８において、暗号化された画像信号を受像機３００に送信する。

受像機３００は、ステップＳ３０８において、暗号化された画像信号を受信する。即ち、ＤＶＩレシーバインターフェース回路３７が、画像信号線５３を介してシリアルデータとして送信されるＲＧＢ各チャンネルのディジタル画像信号を受信し、パラレルデータに変換する。次に、ステップＳ３０９において、復号化ＬＳＩ３０のＨＤＣＰ復号化回路３５が、キャッシュメモリ３４に保存されているＨＤＣＰ方式による暗号鍵を用いて、暗号化されたパラレルデータを復号化する。

ステップＳ３１０において、復号化されたディジタル画像信号は、タイミングコントローラ４１を介して液晶パネル４０に出力され、画像が表示される。

本実施形態においては、画像信号を伝送する際に用いられる情報として、画像信号を暗号化したり復号化したりするために用いられる暗号鍵を例にとって説明した。しかしながら、画像信号を送受信する際に用いられる情報は、暗号鍵に限らず、例えば、送受信される画像信号を表示

するために受像機を最適な状態に設定する情報であっても良い。そのような情報としては、画像の出力タイミングの設定情報、ＰＬＬ（phase locked loop）の設定情報、画像サイズや色の補正に用いられる情報等が挙げられる。

次に、本発明の第２の実施形態に係る受信側の装置について説明する。本実施形態に係る受信側の装置は、外部から暗号鍵等の情報を入力する手段をさらに具備するものである。

図７は、本発明の第２の実施形態に係る受信側の装置を用いた画像伝送システムを示すブロック図である。ここでは、外部から暗号鍵等の情報を入力する手段として、受像機５００にＩＣカードを読み書きするカードリーダー／ライター２１を設けている。復号化ＬＳＩ７０のマスターインターフェース回路３８は、所定の暗号鍵が記録されたＩＣカードが受像機３００に挿入されると、ＥＥＰＲＯＭ２０に優先してカードリーダー／ライター２１によって読み出された暗号鍵をキャッシュメモリ３４に記憶させる。その他の構成については、本発明の第１の実施形態に係る受信側の装置と同様である。

なお、外部から暗号鍵等の情報を入力する手段としては、カードリーダー／ライター２１の替わりに、赤外線リモコンによって送信された信号から情報を読み取る赤外線検出ユニットを設けても良い。その場合には、視聴者が、受像機のリモートコントローラ等を操作することにより、暗号鍵等の情報を受像機に入力することができる。

次に、本実施形態に係る受信側の装置を用いて画像を提供する方法について、図７及び図８を参照しながら説明する。この画像提供方法によれば、ホストコンピュータと同様の機能を有するセットトップボックス等に接続された複数のモニタ（受像機）の内で、特定の暗号鍵が供給されたモニタのみが画像を出力することを可能にする。

図８は、本実施形態に係る受信側の装置を用いて画像を提供する方法を示すフローチャートである。

まず、視聴者は、ステップＳ５０１において、画像情報等のコンテンツの提供者に対して、所望のコンテンツの料金を支払うか、料金を支払うことを約束する。これに応じて、提供者は、ステップＳ６０１において、公開鍵が書き込まれたＩＣカードを視聴者に配付する。また、提供者は、ステップＳ６０２において、このような視聴者のためにコンテンツを送信する。

視聴者が、ステップＳ５０２において、ＩＣカードをモニタに挿入すると、ステップＳ５０３において、セットトップボックスは、ＩＣカードに書き込まれた公開鍵を読み取って、公開鍵に基づいて、このモニタを認証するか否かの判断を行う。モニタが認証されると、ステップＳ５０４において、送信されているコンテンツがモニタに受信され、モニタの画面に表示される。ここで、ステップＳ５０３及びステップＳ５０４における動作の詳細については、図６のステップＳ３０２～Ｓ３１０及びステップＳ４０２～４０８に示す動作と同様である。この画像提供方法によれば、コンテンツのために料金を支払った視聴者のみが、そのコンテンツの提供を受けることができる。

なお、この画像提供方法においては、公開鍵を入力する媒体としてＩＣカードを用いたが、視聴者が、受像機のリモートコントローラに備えられたテンキーを用いて公開鍵をモニタに送信しても良いし、ゲーム機のコントローラとＯＳＤ（open software description）とを用いて公開鍵をモニタに入力しても良い。この他、コンテンツの提供者又は視聴者が、電話回線を用いて公開鍵を配布しても良い。

次に、本発明の第１の実施形態に係る送信側の装置について説明する。これまで、ＨＤＣＰ技術は、パーソナルコンピュータにおいて使用さ

れることが前提となっていた。パーソナルコンピュータが画像信号を暗号化して送信するためには、パーソナルコンピュータのＤＶＩトランスミッタインターフェース回路と、モニタのＤＶＩレシーバインターフェース回路との間で公開鍵の通信を行って、モニタを認証するか否かの判断を行わなくてはならない。その後、パーソナルコンピュータは画像信号の暗号化を開始し、モニタは画像信号の復号化を開始する。この一連の制御動作は、ＨＤＣＰ方式のダウンストリームと呼ばれている。

ここで、パーソナルコンピュータは、ワードプロセッサや表計算のソフトウエアが稼動している場合には画像信号を暗号化する必要がなく、ＤＶＤディスクを再生する場合等に限って画像信号を暗号化する必要が生じる。また、モニタがＨＤＣＰ方式に対応していない場合には、ＤＶＤディスクを再生できない等の表示を行うか、画質を低下させて再生するといった処理を行わなくてはならない。このような制御動作は、オペレーションソフトとグラフィックアクセラレータに内蔵されているＨＤＣＰ制御回路との連携で行われ、ＨＤＣＰ方式のアップストリームと呼ばれている。

このように、従来の送信側の装置においては、送信側の暗号化ＬＳＩと受信側の復号化ＬＳＩだけでは画像信号の伝送制御を行うことができず、外部のソフトウエアの助けを必要としたため、セキュリティに関して問題があった。本実施形態に係る送信側の装置は、このような問題を解決したものである。

図９は、本発明の第１の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。受信側の装置については、図２に示す受像機３００と同一である。送信側の装置６００は、ＤＶＤディスク等から画像信号を再生する画像信号再生回路６０１と、暗号鍵を記憶するための記憶部６０２と、記憶部６０２に記憶されている暗号鍵を用

いて、画像信号再生回路６０１によって再生された画像信号を暗号化して受像機３００に送信する暗号化ＬＳＩ８０とを含んでいる。

暗号化ＬＳＩ８０は、画像信号に所定の信号処理を施す画像処理回路８１と、画像信号再生回路６０１から出力される画像信号と画像処理回路８１から出力される画像信号との内の一方を選択する選択回路８２と、選択回路８２によって選択された画像信号を暗号化する暗号化回路８３と、暗号化回路８３によって暗号化された画像信号を送信する物理層回路８４と、暗号化制御回路８５とを内蔵している。

暗号化制御回路８５は、受信した暗号鍵に基づいて受信側の装置を認証するか否かについて判断し、受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように選択回路８２及び暗号化回路８３を制御し、受信側の装置が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように選択回路８２及び暗号化回路８３を制御する。

次に、本実施形態に係る送信側の装置の動作について詳しく説明する。

送信側の装置６００に電源が投入されると、暗号化制御回路８５は、ＤＶＩケーブル５０の電源線５７を介して受像機３００の一部の回路に電源を投入し、受像機３００のＥＥＰＲＯＭからＥＤＩＤを読み出す。これにより、受像機３００にとって最適な画像信号を知ることができる。ＥＤＩＤを読み出せなかった場合や、ＥＤＩＤを読み出せてもＨＤＣＰ方式に対応していない受像機であると判断した場合には、暗号化制御回路８５は、保護を必要とするコンテンツを送信できないと判断する。

暗号化制御回路８５は、受像機３００がＨＤＣＰ方式に対応していると判断すると、暗号化回路８３と受像機３００のＨＤＣＰ復号化回路を制御して、ＨＤＣＰ方式による受像機の認証を開始する。具体的には、

暗号化制御回路８５が、受信した公開鍵とホスト側の公開鍵とに基づいて、乱数と秘密鍵とを用いた演算を行い、演算結果が一致した場合に、受像機を認証する。

受像機が認証されると、暗号化制御回路８５は、画像再生回路６０１から出力される画像信号を選択するように選択回路８２を制御し、暗号化回路８３に画像信号の暗号化を開始させる。なお、暗号化制御回路８５は、ホットプラグ信号線５８によって、受像機３００に電源が投入されているか否かを検知して、受像機３００に電源が投入されるまで画像信号の送信を行わないようにしても良い。

一方、受像機の認証が所定の時間内に完了しなかった場合には、暗号化制御回路８５は、画像処理回路８１を活性化させ、画像処理回路８１から出力される画像信号を選択するように選択回路８２を制御し、暗号化回路８３に画像信号を平文のまま出力させる。画像処理回路８１は、入力される画像信号の解像度を低下させる処理を施したり、入力される画像信号にノイズを混入させる処理を施したり、入力される画像信号の替わりにコンテンツを送信できない旨のコメントを表す画像信号を出力したりする。これにより、受信側の装置が認証されなかった場合には、受像機３００の画面において、保護する必要のない低品位の画像を表示したり、コンテンツを送信できない旨のコメントを表示したりすることができる。

次に、本発明の第２の実施形態に係る送信側の装置について説明する。本実施形態においては、選択回路を暗号化回路の後段に配置しており、この点が図９に示す装置と異なっている。

図１０は、本発明の第２の実施形態に係る送信側の装置を用いた画像伝送システムを示すブロック図である。受信側の装置については、図２に示す受像機３００と同一である。

送信側の装置７００に含まれている暗号化ＬＳＩ９０は、画像再生回路６０１から出力された画像信号を暗号化する暗号化回路９１と、画像再生回路６０１から出力された画像信号に所定の信号処理を施す画像処理回路９２と、暗号化回路９１から出力される画像信号と画像処理回路９２から出力される画像信号との内の一方を選択する選択回路９３と、選択回路９３によって選択された画像信号を送信する物理層回路９４と、暗号化制御回路９５とを内蔵している。

暗号化制御回路９５は、受信した暗号鍵に基づいて受像機３００を認証するか否かについて判断し、受像機３００が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように選択回路９３を制御し、受像機３００が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように選択回路９３を制御する。

次に、本実施形態に係る送信側の装置の動作について詳しく説明する。

暗号化制御回路９５は、受像機３００がＨＤＣＰ方式に対応していると判断すると、暗号化回路９１と受像機３００のＨＤＣＰ復号化回路を制御して、ＨＤＣＰ方式による受像機の認証を開始する。受像機が認証されると、暗号化制御回路９５は、暗号化回路９１に画像再生回路６０１から出力される画像信号の暗号化を開始させ、暗号化回路９１から出力される画像信号を選択するように選択回路９３を制御する。

一方、受像機の認証が所定の時間内に完了しなかった場合には、暗号化制御回路９５は、画像処理回路９２を活性化させ、画像処理回路９２から出力される画像信号を選択するように選択回路９３を制御する。これにより、受信側の装置が認証されなかった場合には、受像機３００の画面において、保護する必要のない低品位の画像を表示したり、コンテ

ンツを送信できない旨のコメントを表示したりすることができる。

以上、本発明を実施形態に基づいて説明したが、本発明は上記の実施形態に限定されることなく、特許請求の範囲に記載される範囲内で自由に変形及び変更することが可能である。

産業上の利用可能性

本発明は、画像信号を暗号化して送信するコンピュータ等の送信側の装置、及び、暗号化された画像信号を受信して復号化するモニタやプロジェクタ等の受信側の装置において利用することが可能である。さらに、本発明は、そのような受像機を用いて画像を提供するビジネスにおいて利用することが可能である。

請 求 の 範 囲

1．暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、

外部とシリアル通信を行うインターフェース回路と、

前記インターフェース回路によって外部に送信される第１の情報、及び、暗号化された画像信号を復号化するために用いられる第２の情報を書き込み、及び／又は、読み出すように不揮発性メモリを制御するメモリ制御回路と、

を具備する半導体集積回路。

2．前記第１の情報が、前記装置に関するＥＤＩＤ（extended display identification data）を含む、請求項１記載の半導体集積回路。

3．前記第２の情報が、画像信号を復号化するために用いられる暗号鍵を含む、請求項１記載の半導体集積回路。

4．前記不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化回路をさらに具備する請求項３記載の半導体集積回路。

5．外部から供給された暗号鍵を暗号化する暗号鍵暗号化回路をさらに具備する、請求項４記載の半導体集積回路。

6．前記暗号鍵暗号化回路が、画像信号の暗号化強度と同等以上の暗号化強度で暗号鍵を暗号化する、請求項５記載の半導体集積回路。

7．前記暗号鍵暗号化回路が、前記半導体集積回路に所定のコマンドが入力されたときに活性化される、請求項５記載の半導体集積回路。

8．前記メモリ制御回路が、前記不揮発性メモリに情報が正しく書き込まれたか否かをチェックするために、エラー検出コード又はエラー訂正コードを計算して前記不揮発性メモリに書き込まれた情報を検証する、

請求項１記載の半導体集積回路。

９．前記不揮発性メモリをさらに具備する請求項１記載の半導体集積回路。

１０．前記不揮発性メモリに記憶されている内容を一時的に保存するメモリをさらに具備する請求項１記載の半導体集積回路。

１１．暗号化された画像信号を受信する受信回路と、

前記不揮発性メモリに記憶されている第２の情報を用いて、前記受信回路によって受信された画像信号を復号化する画像信号復号化回路と、をさらに具備する請求項１記載の半導体集積回路。

１２．前記画像信号復号化回路が、ＨＤＣＰ（high bandwidth digital content protection）に準拠する方式で暗号化された画像信号を復号化する、請求項１１記載の半導体集積回路。

１３．暗号化された画像信号を受信する装置において用いるための半導体集積回路であって、

不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化回路と、

前記暗号鍵復号化回路によって復号化された暗号鍵を用いて画像信号を復号化する画像信号復号化回路と、

を具備する半導体集積回路。

１４．画像信号を暗号化して受信側の装置に送信する装置において用いるための半導体集積回路であって、

画像信号に所定の信号処理を施す画像処理回路と、

所定の信号処理が施されていない画像信号と所定の信号処理が施された画像信号との内の一方を選択する選択回路と、

前記選択回路によって選択された画像信号を暗号化する暗号化回路と

受信側の装置から受信した暗号鍵に基づいて前記受信側の装置を認証するか否かについて判断し、前記受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように前記選択回路及び前記暗号化回路を制御し、前記受信側の装置が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように前記選択回路及び前記暗号化回路を制御する制御回路と、

を具備する半導体集積回路。

１５．画像信号を暗号化して受信側の装置に送信する装置において用いるための半導体集積回路であって、

画像信号を暗号化する暗号化回路と、

画像信号に所定の信号処理を施す画像処理回路と、

暗号化された画像信号と所定の信号処理が施された画像信号との内の一方を選択する選択回路と、

受信側の装置から受信した暗号鍵に基づいて前記受信側の装置を認証するか否かについて判断し、前記受信側の装置が認証された場合には、所定の信号処理が施されていない画像信号を暗号化して出力するように前記選択回路を制御し、前記受信側の装置が認証されなかった場合には、所定の信号処理が施された画像信号を暗号化しないで出力するように前記選択回路を制御する制御回路と、

を具備する半導体集積回路。

１６．暗号化された画像信号を受信する装置であって、

外部とシリアル通信を行う第１の手段と、

暗号化された画像信号を受信する第２の手段と、

前記第１の手段によって外部に送信される第１の情報、及び、前記第２の手段によって受信された画像信号を復号化するために用いられる第

２の情報を記憶するための不揮発性メモリと、

前記不揮発性メモリに記憶されている第２の情報を用いて、前記第２の手段によって受信された画像信号を復号化する第３の手段と、

を具備する装置。

１７．前記不揮発性メモリが、前記装置に関するＥＤＩＤ（extended display identification data）を第１の情報として記憶する、請求項１６記載の装置。

１８．前記不揮発性メモリが、画像信号を復号化するために用いられる暗号鍵を第２の情報として記憶する、請求項１６記載の装置。

１９．前記不揮発性メモリが、暗号化された暗号鍵を第２の情報として記憶し、

前記装置が、前記不揮発性メモリに記憶されている暗号化された暗号鍵を復号化する暗号鍵復号化手段をさらに具備する、請求項１８記載の装置。

２０．外部から供給された暗号鍵を暗号化する暗号鍵暗号化手段をさらに具備する、請求項１９記載の装置。

２１．前記不揮発性メモリが、シリアルＥＥＰＲＯＭ（electrically erasable programmable read-only memory）を含む、請求項１６記載の装置。

２２．前記不揮発性メモリを制御するためのマイクロコンピュータをさらに具備する請求項１６記載の装置。

２３．前記不揮発性メモリに記憶されている内容を一時的に保存するメモリをさらに具備する請求項１６記載の装置。

２４．前記第３の手段が、ＨＤＣＰ（high bandwidth digital content protection）に準拠する方式で暗号化された画像信号を復号化する、請求項１６記載の装置。

２５．暗号化された画像信号を受信する装置であって、

暗号鍵を入力する第１の手段と、

暗号化された画像信号を受信する第２の手段と、

前記第１の手段によって入力された暗号鍵を用いて、前記第２の手段によって受信された画像信号を復号化する第３の手段と、

を具備する装置。

２６．前記第１の手段が、ＩＣカードに記憶された情報を読み取る、請求項２５記載の装置。

２７．前記第１の手段が、赤外線リモコンによって送信された信号から情報を読み取る、請求項２５記載の装置。

２８．外部とシリアル通信を行う第１の手段と、暗号化された画像信号を受信する第２の手段と、不揮発性メモリとを有し、暗号化された画像信号を受信する装置を製造する方法であって、

前記第１の手段を用いてシリアル通信を行うことにより、前記装置に関する第１の情報、及び、前記第２の手段によって受信された画像信号を復号化するために用いられる第２の情報を前記装置に入力するステップ（ａ）と、

ステップ（ａ）において入力された第１及び第２の情報を前記不揮発性メモリに書き込むステップ（ｂ）と、

を具備する方法。

２９．ステップ（ａ）とステップ（ｂ）との間において、第２の情報を暗号化するステップをさらに具備する請求項２８記載の方法。

３０．前記第１の手段を用いてシリアル通信を行うことにより、ステップ（ｂ）において前記不揮発性メモリに書き込んだ情報を確認するステップをさらに具備する請求項２８記載の方法。

３１．外部とシリアル通信を行う第１の手段と、暗号化された画像信号

を受信する第２の手段と、不揮発性メモリとを有し、暗号化された画像信号を受信する装置を修理する方法であって、

前記第１の手段を用いてシリアル通信を行うことにより、前記装置に関する第１の情報、及び、前記第２の手段によって受信された画像信号を復号化するために用いられる第２の情報を前記装置に入力するステップ（ａ）と、

ステップ（ａ）において入力された第１及び第２の情報を用いて、前記不揮発性メモリに記憶されている情報を書き替えるステップ（ｂ）と、

を具備する方法。

３２．ステップ（ａ）とステップ（ｂ）との間において、第２の情報を暗号化するステップをさらに具備する請求項３１記載の方法。

３３．暗号鍵を入力する第１の手段と、暗号化された画像信号を受信する第２の手段とを有し、暗号化された画像信号を受信して画像を表示する受像機を用いて画像を提供する方法であって、

前記第１の手段によって受像機に入力された暗号鍵に基づいて、前記受像機を認証するか否かについて判断するステップ（ａ）と、

ステップ（ａ）において前記受像機が認証された場合に、前記第２の手段によって受信された画像信号を前記第１の手段によって受像機に入力された暗号鍵を用いて復号化し、復号化された画像信号に基づいて画像を表示するステップ（ｂ）と、

を具備する方法。

FIG.1

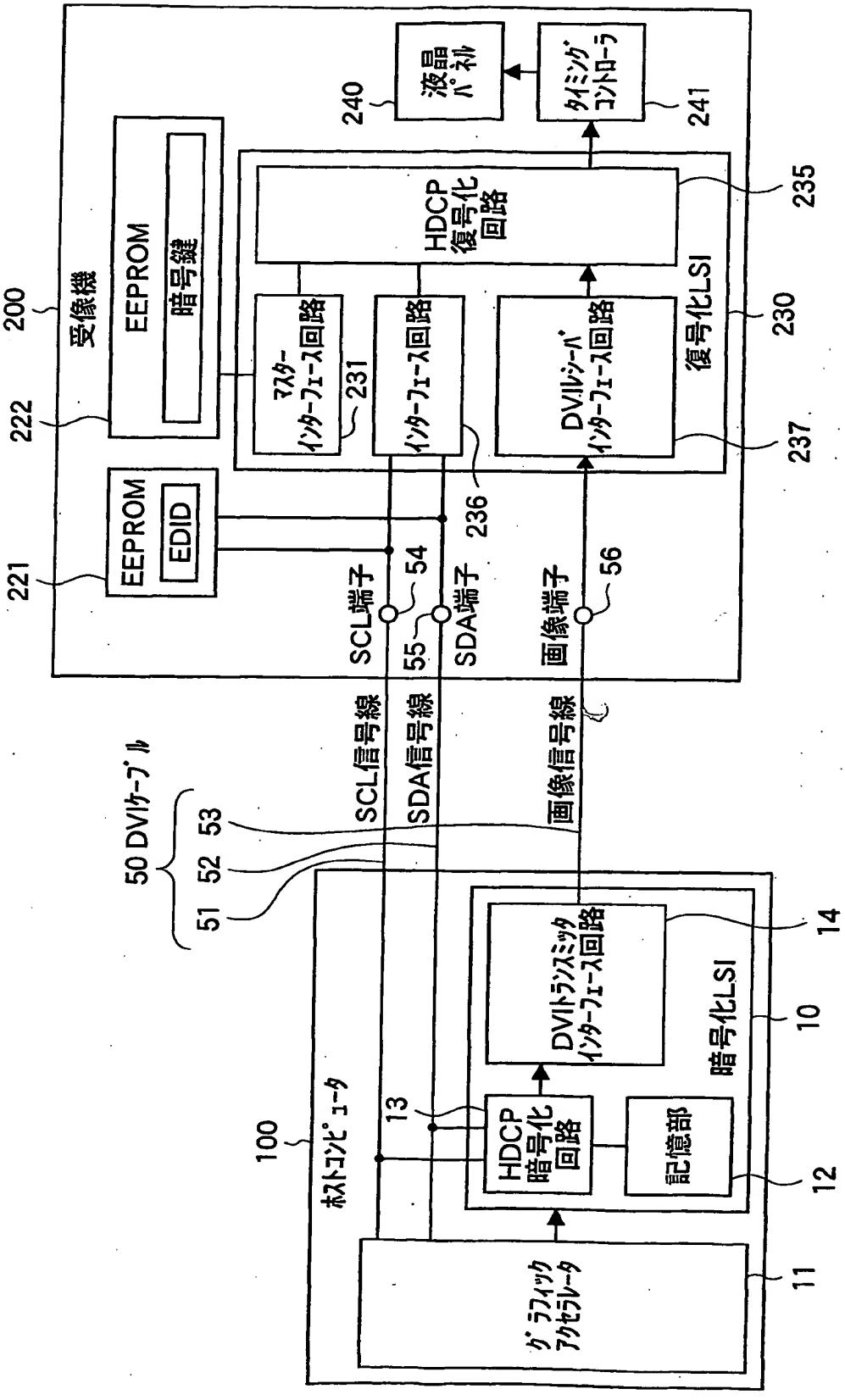

受像機
200
EEPROM
暗号鍵
222
EEPROM
EDID
221
液晶パネル
240
タイミングコントローラ
241
HDCP復号化回路
235
マスターインターフェース回路
231
インターフェース回路
236
DVレシーバインターフェース回路
237
復号化LSI
230
SCL端子
54
SDA端子
55
画像端子
56
SCL信号線
SDA信号線
画像信号線
50 DVケーブル
53
52
51
ホストコンピュータ
100
13
HDCP暗号化回路
記憶部
12
DVトランスミッタインターフェース回路
14
暗号化LSI
10
グラフィックアクセラレータ
11

FIG.2

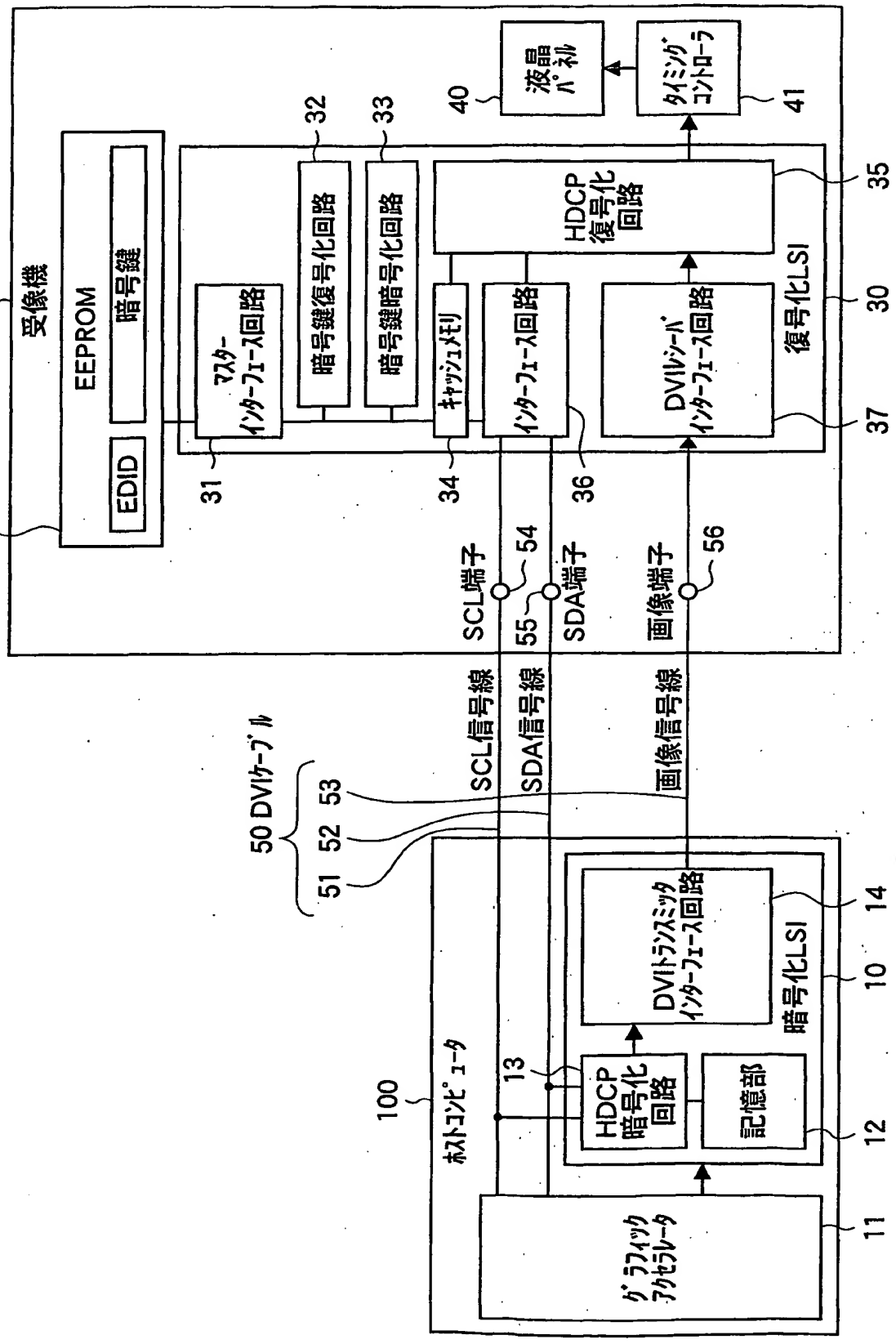

受像機
300
EEPROM
暗号鍵
EDID
20
マスター
インターフェース回路
31
暗号鍵復号化回路
32
暗号鍵暗号化回路
33
キャッシュメモリ
34
インターフェース回路
36
HDCP
復号化
回路
35
DVIレシーバ
インターフェース回路
37
復号化LSI
30
液晶
パネル
40
タイミング
コントローラ
41
SCL端子
54
SDA端子
55
画像端子
56
SCL信号線
SDA信号線
画像信号線
50 DVIケーブル
53
52
51
ホストコンピュータ
100
グラフィック
アクセラレータ
11
HDCP
暗号化
回路
13
記憶部
12
DVIトランスミッタ
インターフェース回路
14
暗号化LSI
10

FIG.3

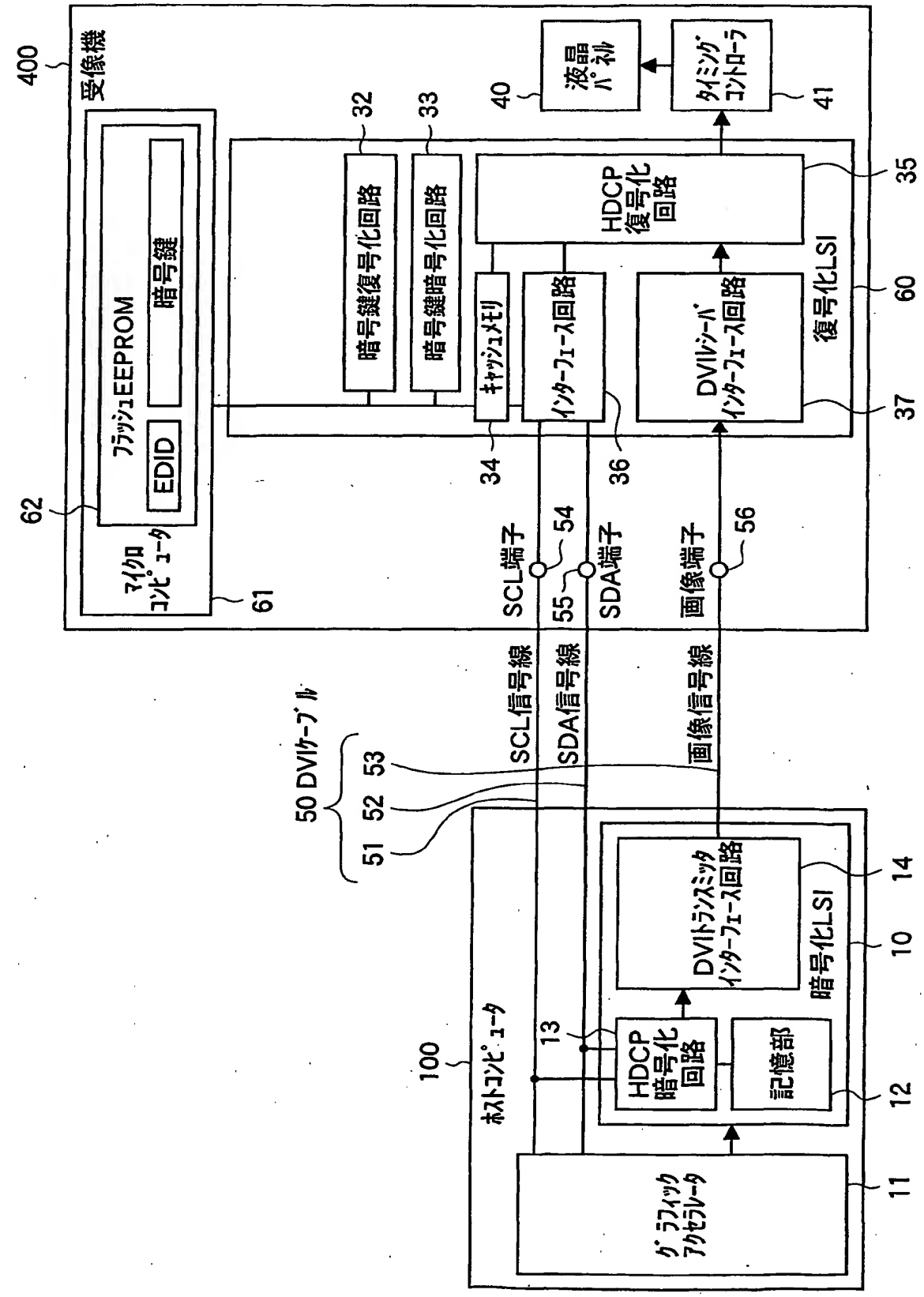

400
受像機
62
フラッシュEEPROM
暗号鍵
EDID
マイクロコンピュータ
61
32
33
40
液晶パネル
タイミングコントローラ
41
暗号鍵復号化回路
暗号鍵暗号化回路
HDCP復号化回路
35
キャッシュメモリ
インターフェース回路
DVIレシーバインターフェース回路
復号化LSI
60
37
34
36
SCL端子
54
SDA端子
55
画像端子
56
SCL信号線
SDA信号線
画像信号線
50 DVIケーブル
53
52
51
100
ホストコンピュータ
13
HDCP暗号化回路
記憶部
DVIトランスミッタインターフェース回路
暗号化LSI
14
10
12
グラフィックアクセラレータ
11

FIG.4

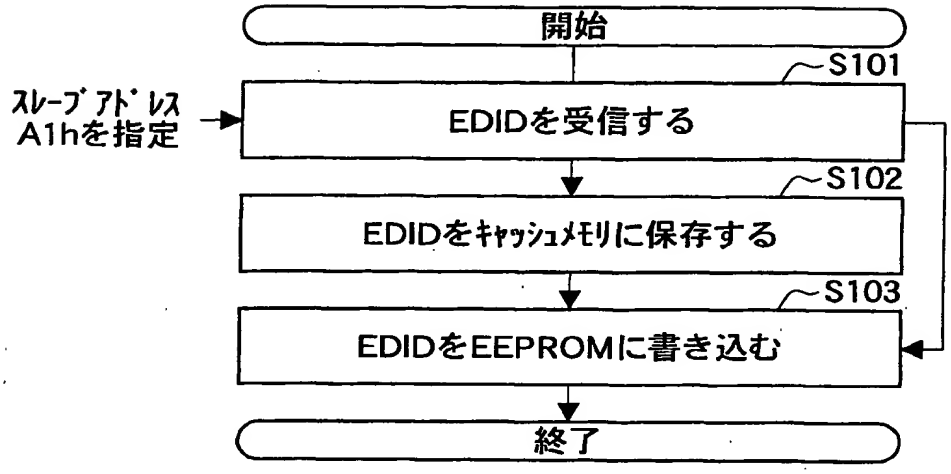

開始
S101
スレーブアドレス
A1hを指定
EDIDを受信する
S102
EDIDをキャッシュメモリに保存する
S103
EDIDをEEPROMに書き込む
終了

FIG.5

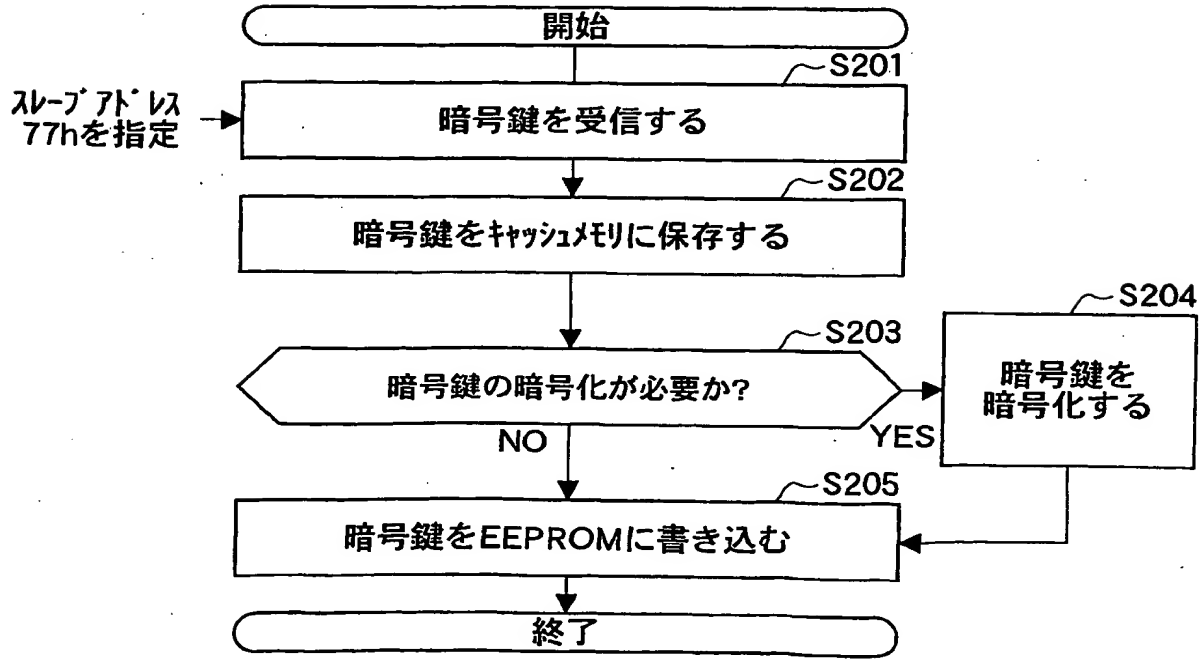

開始
S201
スレーブアドレス
77hを指定
暗号鍵を受信する
S202
暗号鍵をキャッシュメモリに保存する
S204
S203
暗号鍵の暗号化が必要か?
暗号鍵を
暗号化する
NO
YES
S205
暗号鍵をEEPROMに書き込む
終了

FIG.6

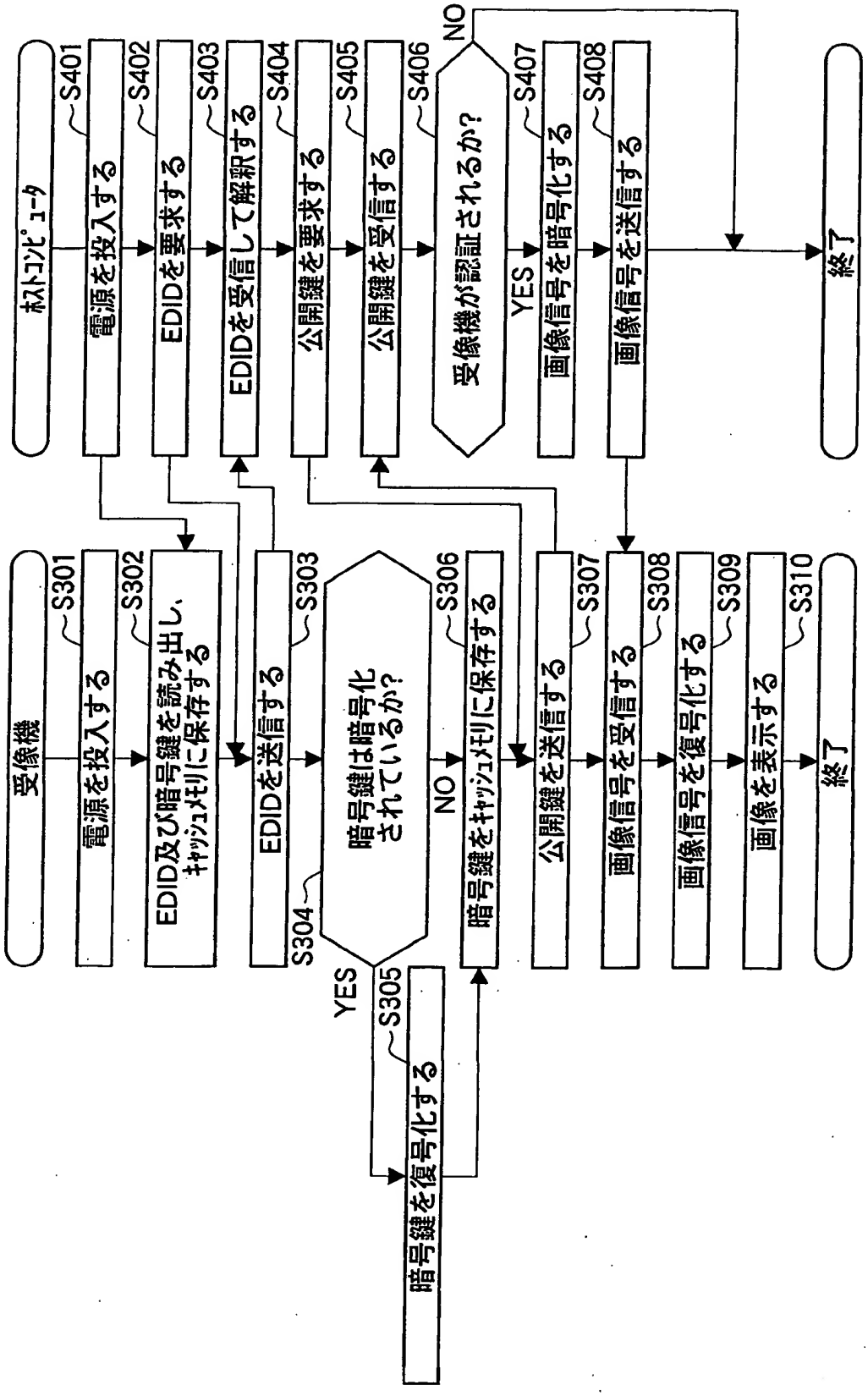

パソコン
電源を投入する
S401
EDIDを要求する
S402
EDIDを受信して解釈する
S403
公開鍵を要求する
S404
公開鍵を受信する
S405
受像機が認証されるか?
S406
NO
YES
画像信号を暗号化する
S407
画像信号を送信する
S408
終了
受像機
電源を投入する
S301
EDID及び暗号鍵を読み出し、キャッシュメモリに保存する
S302
EDIDを送信する
S303
暗号鍵は暗号化されているか?
S304
YES
暗号鍵を復号化する
S305
NO
暗号鍵をキャッシュメモリに保存する
S306
公開鍵を送信する
S307
画像信号を受信する
S308
画像信号を復号化する
S309
画像を表示する
S310
終了

FIG.7

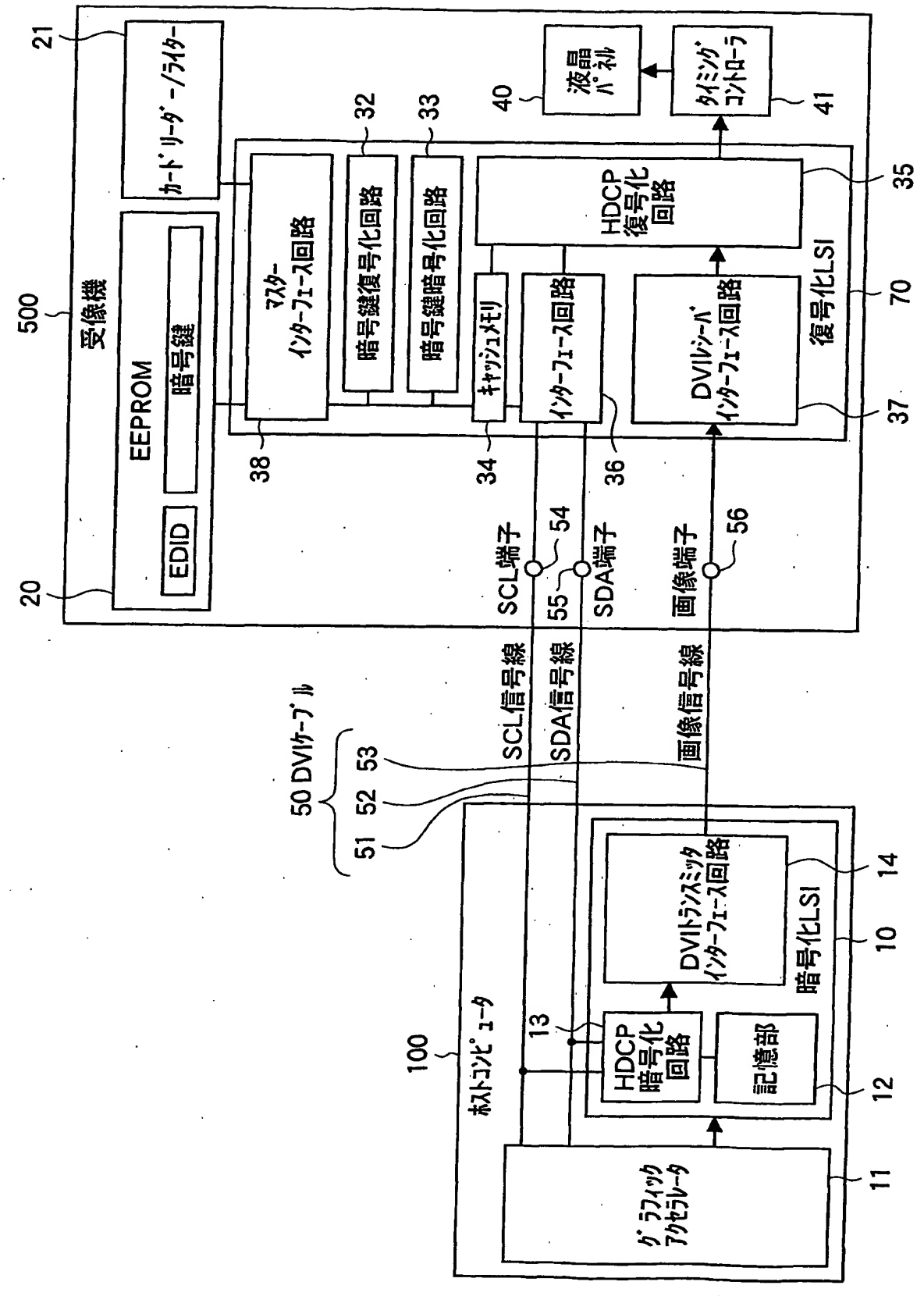

受像機
500
EEPROM
暗号鍵
EDID
20
カードリーダ・ライター
21
マスター
インターフェース回路
38
暗号鍵復号化回路
32
暗号鍵暗号化回路
33
キャッシュメモリ
34
インターフェース回路
36
HDCP
復号化
回路
35
DVIレシーバ
インターフェース回路
37
復号化LSI
70
液晶
パネル
40
タイミング
コントローラ
41
SCL端子
54
SDA端子
55
画像端子
56
50 DVIケーブル
51
52
53
SCL信号線
SDA信号線
画像信号線
ホストコンピュータ
100
グラフィック
アクセラレータ
11
HDCP
暗号化
回路
13
記憶部
12
DVIトランスミッタ
インターフェース回路
14
暗号化LSI
10

FIG.8

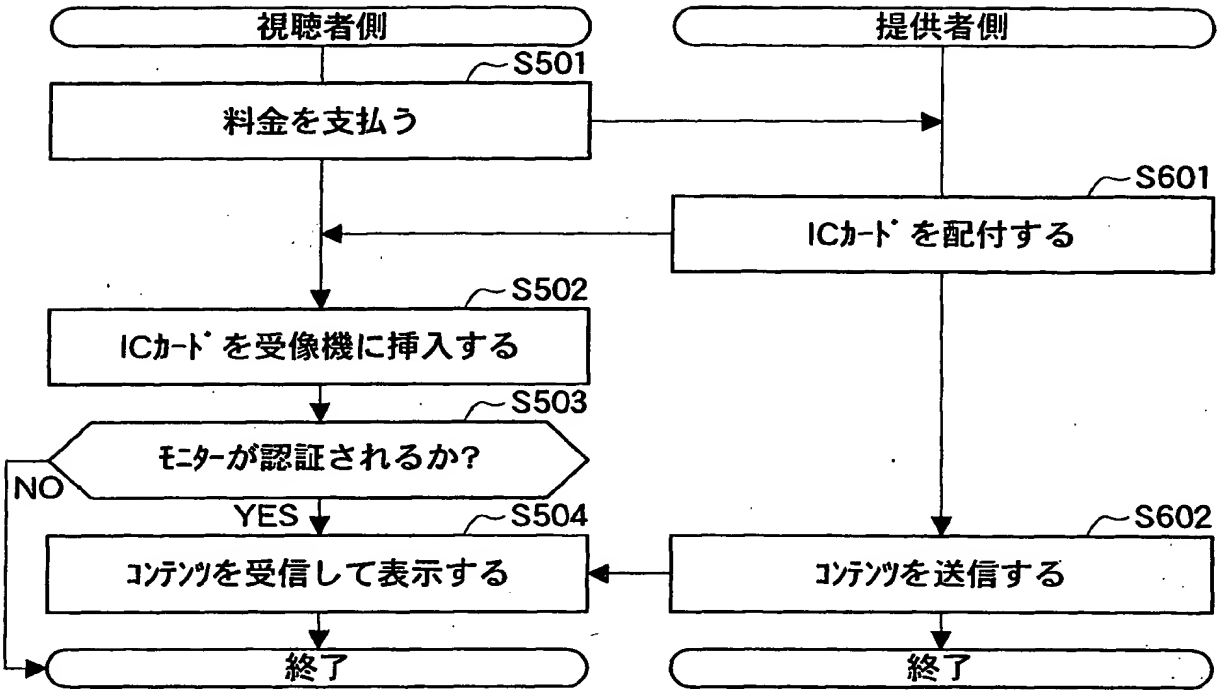

視聴者側
提供者側
S501
料金を支払う
S601
ICカード を配付する
S502
ICカード を受像機に挿入する
S503
モニターが認証されるか?
NO
YES
S504
コンテンツを受信して表示する
S602
コンテンツを送信する
終了
終了

FIG.9

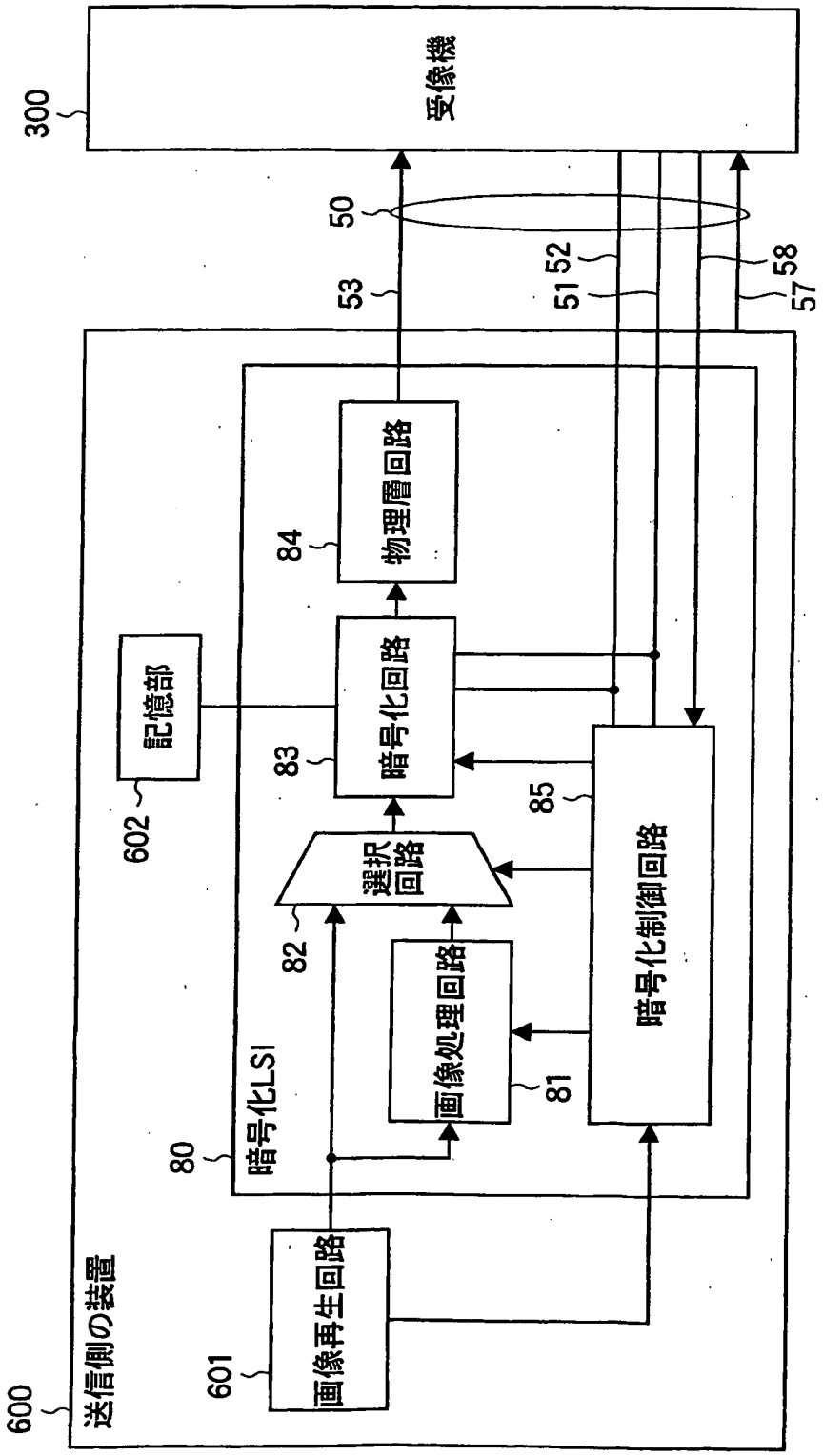
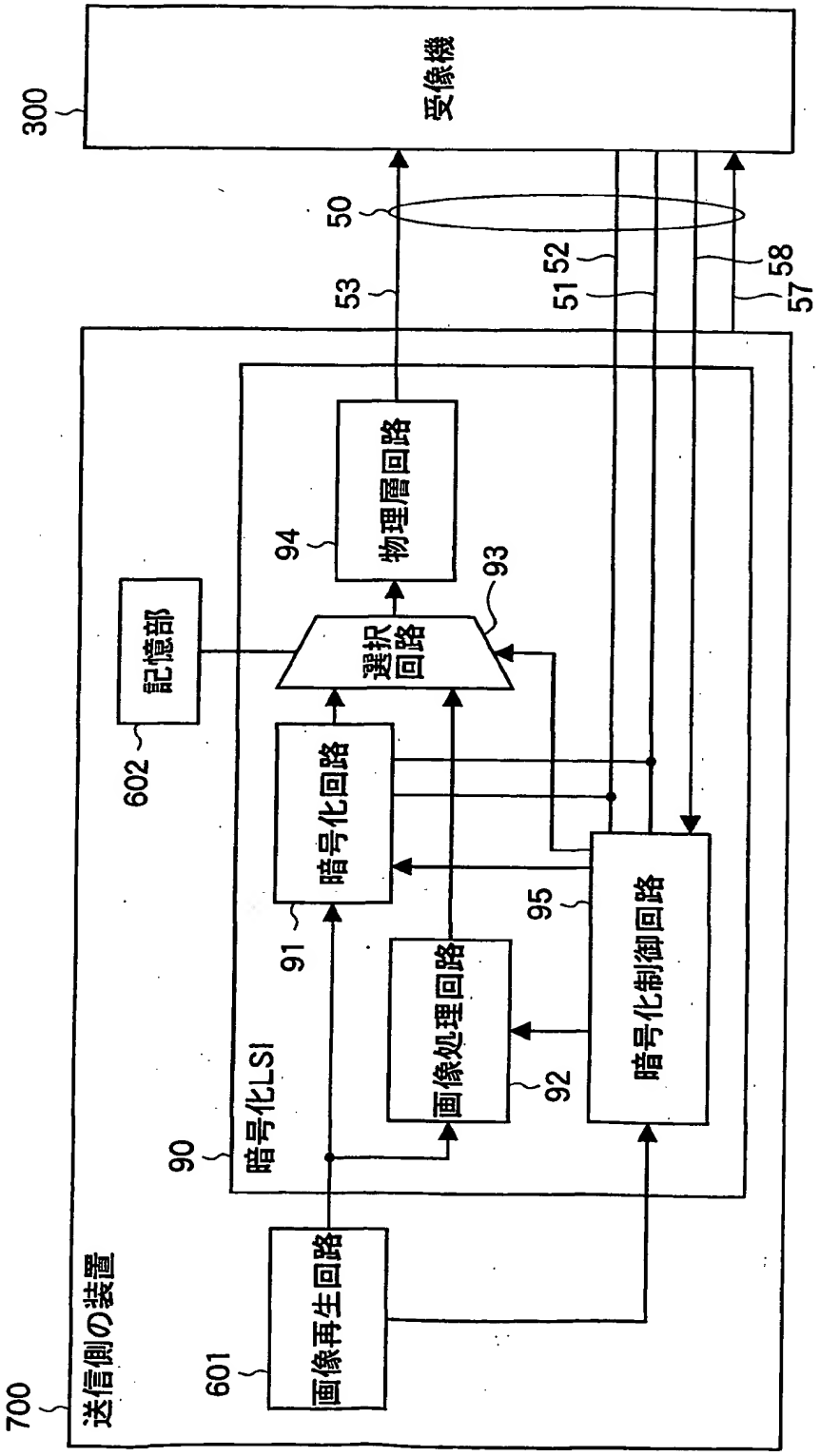

300
受像機
50
53
51
52
57
58
600
送信側の装置
601
画像再生回路
80
暗号化LSI
602
記憶部
82
選択回路
81
画像処理回路
85
暗号化制御回路
83
暗号化回路
84
物理層回路

FIG.10


300
受像機
50
53
51
52
57
58
送信側の装置
700
暗号化LSI
90
601
画像再生回路
602
記憶部
91
暗号化回路
92
画像処理回路
93
選択回路
94
物理層回路
95
暗号化制御回路

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/09279

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G09G 5/00, H04N 7/16,
H04N 1/00, H04N 1/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G09G 5/00, H04N 7/16,
H04N 1/00, H04N 1/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2002
Kokai Jitsuyo Shinan Koho 1971-2002 Toroku Jitsuyo Shinan Koho 1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	High-bandwidth Digital Content Protection. WHITE PAPER. [online]. Silicon Image, Inc. February 2000. [retrieved on 2002-01-11]. Retrieved from the Internet: <URL: http://www.siimage.com/documents/ SiI-WP-002-A.pdf>.	1-33
Y	JP 11-73375 A (Dainippon Printing Co., Ltd.), 16 March, 1999 (16.03.1999), Full text; Figs. 1 to 5 (Family: none)	1-33
Y	JP 2000-181802 A (Matsushita Electric Ind. Co., Ltd.), 30 June, 2000 (30.06.2000), Full text; Figs. 1 to 5 (Family: none)	1-33
Y	JP 8-185361 A (Hitachi, Ltd.), 16 July, 1996 (16.07.1996), Full text; Figs. 1 to 4 (Family: none)	1-33
Y	WO 99/07150 A (SCIENTIFIC-ATLANTA, INC.), 11 February, 1999 (11.02.1999), Full text; Figs. 1 to 29 & JP 2001-512842 A	1-33

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
15 January, 2002 (15.01.02)

Date of mailing of the international search report
29 January, 2002 (29.01.02)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/09279

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-194603 A (Dainippon Printing Co., Ltd.), 14 July, 2000 (14.07.2000), Full text; Figs. 1 to 7 (Family: none)	4-7,19,20
Y	JP 8-6879 A (Toshiba Corporation), 12 January, 1996 (12.01.1996), Full text; Figs. 1 to 4 (Family: none)	14,15,33
Y	JP 6-197104 A (Sony Corporation), 15 July, 1994 (15.07.1994), Full text; Figs. 1 to 5 (Family: none)	26
Y	JP 9-97216 A (Sony Corporation), 08 April, 1997 (08.04.1997), Full text; Fig. 16 (Family: none)	27
Y	JP 2000-194346 A (NEC Home Electronics Ltd.), 14 July, 2000 (14.07.2000), Full text; Figs. 1 to 3 (Family: none)	28-32

国際調査報告

国際出願番号 PCT／JP01／09279

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷ G06F12／14, G09G 5／00, H04N 7／16,
H04N 1／00, H04N 1／44

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷ G06F12／14, G09G 5／00, H04N 7／16,
H04N 1／00, H04N 1／44

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1922 － 1996年
日本国公開実用新案公報 1971 － 2002年
日本国実用新案登録公報 1996 － 2002年
日本国登録実用新案公報 1994 － 2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	High-bandwidth Digital Content Protection. WHITE PAPER. [online]. Silicon Image, Inc. February 2000. [retrieved on 2002-01-11]. Retrieved from the Internet: <URL: http://www.siimage.com/documents/SiI-WP-002-A.pdf>.	1－33
Y	JP 11－73375 A（大日本印刷株式会社） 1999. 03. 16, 全文, 第1－5図（ファミリーなし）	1－33

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 15. 01. 02

国際調査報告の発送日 29.01.02

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員） 5N 3044
相崎 裕恒
電話番号 03－3581－1101 内線 3585

国際調査報告

国際出願番号 PCT／JP01／09279

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2000－181802 A（松下電器産業株式会社） 2000．06．30，全文，第1－5図（ファミリーなし）	1－33
Y	JP 8－185361 A（株式会社日立製作所） 1996．07．16，全文，第1－4図（ファミリーなし）	1－33
Y	WO 99／07150 A （SCIENTIFIC－ATLANTA，INC．） 1999．02．11，全文，第1－29図 & JP 2001－512842 A	1－33
Y	JP 2000－194603 A（大日本印刷株式会社） 2000．07．14，全文，第1－7図（ファミリーなし）	4－7，19，20
Y	JP 8－6879 A（株式会社東芝） 1996．01．12，全文，第1－4図（ファミリーなし）	14，15，33
Y	JP 6－197104 A（ソニー株式会社） 1994．07．15，全文，第1－5図（ファミリーなし）	26
Y	JP 9－97216 A（ソニー株式会社） 1997．04．08，全文，第16図（ファミリーなし）	27
Y	JP 2000－194346 A （日本電気ホームエレクトロニクス株式会社） 2000．07．14，全文，第1－3図（ファミリーなし）	28－32